



Security & YOU

Think.
Assess.
Protect.

Learning Minute: **OUO and You**

Based on true stories from real life at SNL

What do you think?

Jesse and email

Jesse needed to do some work at home over the weekend to meet a deadline. Since it was OOU, he emailed the file to himself at his *sandia.gov* address. At home, he used his cryptocard to log into his email. He saved the file to his personal computer's desktop, worked on the document, and then used the same Sandia email to send it back to himself at the office.

Julie and the DropZone

Julie needed to share some OOU files with her colleagues. Because there were several files, Julie created a folder on the DropZone to house the documents, and sent the link to her peers.

What did they do wrong? DISCUSS.

Answers

Jesse and Email

Jesse should not have saved Sandia information to his personal computer. It would have been better if he had remoted in to his SNL desktop and did the work from there. The Data Loss Prevention tool didn't stop the email because it was sent to a *sandia.gov* address.

Julie and the DropZone

Julie should have put passwords on the documents or used the Protected DropZone to share sensitive files. Anyone at SNL has access to the regular DropZone, including foreign nationals.

The Risk

- Both Jesse and Julie left information where it could be accessible to others who do not have a need to know (family members, anyone with access to the DropZone).
- Even unclassified information has value to our adversaries. Add protections to keep the information safe.

Protect (Learning Points)

Protection in Use

- Each of us is responsible for ensuring protective measures are in place when accessing and using OUO.
- “Reasonable precautions” must be taken to prevent access by persons who do not require OUO information to perform their jobs or other DOE-authorized activities (e.g., don’t read an OUO document in a public place).

Protect (Learning Points)

Protection in Storage

- In Limited Areas, OOU should be stored out of sight in receptacles (not required to be locked) such as file cabinets, desks, or bookcases during non-duty hours. An office with a door can serve as the receptacle.*
 - However, OOU Exemption 6, Personal Privacy (e.g., medical, marital status, Social Security numbers, and HR information), **is required** to be stored in a **locked** receptacle.
- In Property Protection Areas or General Access Areas, the receptacles for OOU (including office spaces) must be locked after duty hours.

* During duty hours in a Limited Area, documents containing OOU may be left on desks, but it is a best business practice to turn the documents over or obscure the information from casual passers-by.

Protect (Learning Points)

Protection in Storage, continued...

- It is recommended to only remove from storage the amount of OUO necessary to conduct work.
- SNL/NM uses white destruction bags to collect OUO paper pending destruction. Because of the large amount of information that is potentially of interest to an adversary, Operations Security (OPSEC) principles should be used for the protection of the bags (e.g., protecting bags until pickup).

Protect (Learning Points)

Protection in Transit (Cyber Protections)

- When emailing OUO information, be sure to encrypt it and the attachment (if any) before sending it to an address outside the Sandia firewall (any address other than '@sandia.gov').
 - Emailing within the Sandia domain (all '@sandia.gov addresses) is already encrypted.
- If you need to share OUO with an outside business partner, there are several options available. Go to the Information Protection Options [page](#) to see a list.

Questions?

Phone: 321 (from any Sandia phone) or 845-1321

Web: security.sandia.gov

Email: security@sandia.gov